UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/877,150	06/08/2001	Thomas P. Hardjono	2204/A82	9914

2101 7590 02/28/2005

BROMBERG & SUNSTEIN LLP
125 SUMMER STREET
BOSTON, MA 02110-1618

EXAMINER	
ELMORE, JOHN E	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 02/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/877,150	HARDJONO, THOMAS P.	
	Examiner	Art Unit	
	John Elmore	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,7-11,14-16 and 20* is/are rejected.

7)☒ Claim(s) *5-7, 12-13 and 17-19* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 June 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-20 are examined.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. **Claim 1, 8, and 15 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Gong et al, hereinafter Gong, ("Multicast security and its extension to a mobile environment," Wireless Networks I, 1995), in view of Ko et al, hereinafter Ko, ("Location-Based Multicast in Mobile Ad Hoc Networks," September 3,1998) and further in view of Reudink et al, hereinafter Reudink, (USPN 5,884,147 – published March 16, 1999).

Gong discloses a secure communication system comprising:

a plurality of geographical cells (page 290, column 2, paragraph 4, citing Katz, who discloses a digital cellular network; see Katz; page 13, section 4.2, paragraph 1), each cell being associated with a specific geographic area and having a cell (session key; page 293, section 5.4, paragraph 2); and

a key management center (page 293, section 5.4, paragraph 4) distributes

to the mobile device a set of cryptographic keys necessary to permit secure communication within each cell (page 291, section 5.2, paragraph 3).

But Gong does not explicitly explain that each cell has a cell cryptographic key for secure communications with devices located within the cell.

However, Gong teaches the use of a single cryptographic key (session key) to permit secure communications among devices that belong to the same multicast session (page 293, section 5.4). And Ko teaches a multicast session confined to a cell (specific geographical area) wherein all mobile hosts located within the region would comprise the group (location-based multicast group; see page 2, paragraph 2), reducing communication costs when communicating among hosts within a region (page 1, paragraph 1).

Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Gong such that each cell has a cell cryptographic key for secure communications with devices located within the cell. One would be motivated to do so in order to reduce the communication costs of communicating with hosts within a given cell.

Also beyond the scope of Gong is a key management center that determines an anticipated cell path of a mobile device from a current cell to a destination cell and distributes keys necessary to permit secure communication within each cell along the anticipated path.

However, Reudink teaches a management center (host; column 2, lines 55-65, and column 7, line 25) in the context of a plurality of geographic cells (column 7, lines

21-24) that determines an anticipated cell path of a mobile device from a current cell to a destination cell in order to optimize wireless activity within each cell (column 7, line 66, through column 8, line 12).

Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Gong to enhance the functionality of the key management center to determine an anticipated cell path of a mobile device from a current cell to a destination cell and to distribute a set of cryptographic keys necessary to permit secure communication for the device within each cell along the anticipated path. One would be motivated to do so in order to optimize wireless activity in the cells, particularly improving on the time and effort necessary to register with a base station and obtain from the key management center a new cell key as each cell is entered.

Regarding claim 8, method steps comprising each of these limitations have already been addressed as set forth above (relative to claim 1). Therefore, for reasons applied above, such a claim also would have been obvious.

Regarding claim 15, a product comprising each of these limitations have already been addressed as set forth above (relative to claim 1). Therefore, for reasons applied above, such a claim also would have been obvious.

3. **Claims 2-4, 9-11 and 16 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Gong and Reudink in view of Caronni et al, hereinafter Caronni, (USPN 6,049,878 – published April 11, 2000).

Regarding dependent claim 2, Gong and Reudink are relied upon for teaching in regard to claim 1. But Gong and Reudink do not explain a hierarchical tree having a root node, a plurality of internal nodes, and a plurality of terminal leaf nodes, the root node and each internal node having an associated node cryptographic key for secure communication with lower nodes in the tree, each leaf node being associated with a specific geographic cell.

However, Gong teaches encryption keys for multicasting that are hierarchical, providing access by participants to messages encrypted by keys of all higher levels than their own level (page 290, column 2, paragraph 1). And in regard to multicasting, Caronni teaches a hierarchical tree having a root node, a plurality of internal nodes, and a plurality of terminal leaf nodes, the root node and each internal node having an associated node cryptographic key for secure communication with lower nodes in the tree (column 6, lines 29-50, and Figure 4), as a more efficient means of managing cryptographic keys when the number of keys necessary to facilitate the network activity is large and dynamically changing (column 4, lines 23-28).

Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Gong and Redink to further comprise a hierarchical tree having a root node, a plurality of internal nodes, and a plurality of terminal leaf nodes, the root node and each internal node having an associated node cryptographic key for secure communication with lower nodes in the tree. Each leaf node would be associated with a specific geographic cell because all participants within a cell share a session key (cell key) rather than have their own individual keys. One

would be motivated to do so in order to more efficiently manage cryptographic keys when the number of keys necessary to facilitate the network activity is large and dynamically changing as in the case of a large number of cells in the anticipated path for a mobile device.

Regarding dependent claim 3, Caronni further discloses a system wherein the cryptographic key of each node below the root node is derived by applying a mathematical function to the cryptographic key of the next higher level node (key encryption key; see column 6, lines 29-65, and column 9, lines 10-24).

Regarding dependent claim 4, Caronni further discloses a system wherein the mobile device knows the cryptographic key of each node in the tree on a direct path back to the root node (participants store all the keys in a path from leaf to root (traffic encryption key); see column 6, lines 28-39, and column 8, lines 44-55, and Figure 4).

Regarding claims 9-11, method steps comprising each of these limitations have already been addressed as set forth above (relative to claims 2, 3, 4). Therefore, for reasons applied above, such claims also would have been obvious.

Regarding claim 16, a product comprising each of these limitations have already been addressed as set forth above (relative to claims 1 and 2). Therefore, for reasons applied above, such a claim also would have been obvious.

4. **Claims 7, 14, and 20 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Gong and Reudink in view of Wong et al, hereinafter Wong, ("Secure

Group Communications Using Key Graphs," Computer Communication Review, 1998, as cited in the IDS).

Regarding dependent claim 2, Gong and Reudink teach all the elements of claim1. But Gong and Reudink do not explain a system wherein the set of cryptographic keys contains the minimum number of keys necessary to permit secure communications for the mobile device within each cell along the anticipated cell path, but no other cells.

However, Gong teaches encryption keys for multicasting that are hierarchical, providing access by participants to messages encrypted by keys of all higher levels than their own level (page 290, column 2, paragraph 1). And Wong teaches a method wherein the minimum number of keys in a hierarchical key tree are distributed (see section 2.1) in order to improve scalability (see section 1.1).

Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Gong and Redink with the teaching of Wong wherein the set of cryptographic keys contains the minimum number of keys necessary to permit secure communications for the mobile device within each cell along the anticipated cell path, but no other cells. One would be motivated to do so in order to provide for greater scalability of the system.

Regarding claims 14 and 20, a system comprising each of these limitations have already been addressed as set forth above (relative to claims 1 and 7). Therefore, for reasons applied above, such a claim also would have been obvious.

Allowable Subject Matter

5. **Claims 5-7, 12-14, and 17-20 are objected to as being dependent upon a rejected base claim**, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claims 5, 12, 17, and 18 are allowable because the closest prior art does not teach a system wherein at least one level of the tree uses three-dimensions to connect to nodes in the next lower hierarchical level. Caronni, teaches only a binary hierarchical tree. And Wong et al ("Secure Group Communication Using Key Graphs," February 2000, cited in the IDS), teach n-ary key trees (key stars), but not the use of multiple connected trees that can be used to form the three-dimensional structure claimed.

Claims 6, 13, and 19 are allowable because the closest prior art, Gong and Reudnink, do not teach that session keys are valid for a restricted period time based on the anticipated cell path.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Omar et al, "Multicast Support for Mobile-IP with the Hierarchical Local Registration Approach," Proceedings of WOWMOM'00, August 2000.

Ramjee et al, "IP-Based Access Network Infrastructure for Next-Generation Wireless Data Networks," IEEE Personal Communications, August 2000.

Kruus, P., "A Survey of Multicast Security Issues and Architectures," Naval Research Laboratory Report, 1998.

Campbell et al, "Design, Implementation, and Evaluation of Cellular IP," IEEE Personal Communications, August 2000.

Karagiannis, G., "Mobile IP: State of the Art Report," Ericsson Open Report, July 13, 1999.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John Elmore whose telephone number is 571-272-4224. The examiner can normally be reached on M 10-8, T-Th 9-7.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 703-308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

***

David Y. Jung
Primary Examiner

10/28/04

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100